

1 ABSTRACT

2 Storing events to enhance intrusion detection in networks is described. In  
3 one exemplary implementation, an event is received. The event includes a data  
4 section containing a set of strings each having an event field. A definition table is  
5 referenced to determine locations of event fields in the data section of the event.  
6 The event fields are stored in a database record corresponding to event field  
7 locations referenced from the definition table.

10076039.024302  
2025T20:5503Z001